

(11)Publication number : 2001-292135

(43)Date of publication of application : 19.10.2001

(51)Int.Cl.

H04L 9/08
G09C 1/00
H04L 12/28
H04L 12/22

(21)Application number : 2000-106030

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 07.04.2000

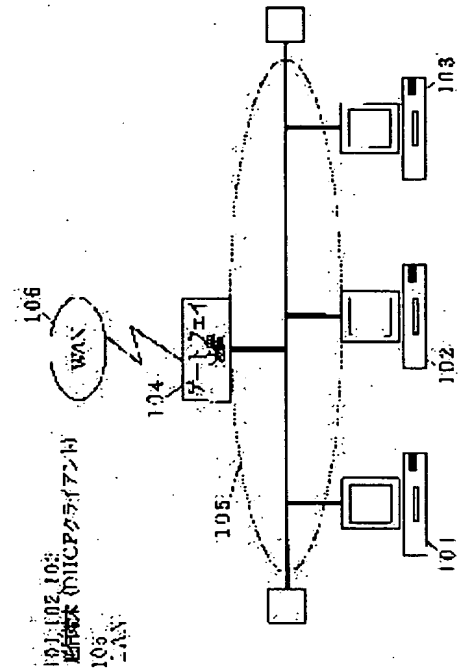
(72)Inventor : MURAKAWA YASUSHI

(54) KEY EXCHANGE SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a key exchange system which can share password key data by allowing a plurality of communication terminals and a gateway device on a LAN to individually and easily exchange key data, by using an existing communication protocol.

SOLUTION: In the key exchange system, having a plurality of communication terminals 101, 102 and 103 connected to the LAN 105 and the gateway device 104 as a DHCP server, which is connected to the LAN and a WAN 106 and which performs concentration/conversion processing, the communication terminals 101, 102 and 103 exchange key data with the gateway device 104, in order to obtain network information at the time of starting DHCP communication.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(51) Int. Cl. ⁷	識別記号	F I	テマコード (参考)
H04L 9/08		G09C 1/00	660 E 5J104
G09C 1/00	660	H04L 9/00	601 C 5K030
H04L 12/28			601 E 5K033
12/22		11/00	310 D 9A001
		11/26	
		審査請求 未請求 請求項の数 4	〇 L (全10頁)

(21) 出願番号 特願2000-106030 (P 2000-106030)

(22) 出願日 平成12年4月7日 (2000.4.7)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 村川 泰

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74) 代理人 100097445

弁理士 岩橋 文雄 (外2名)

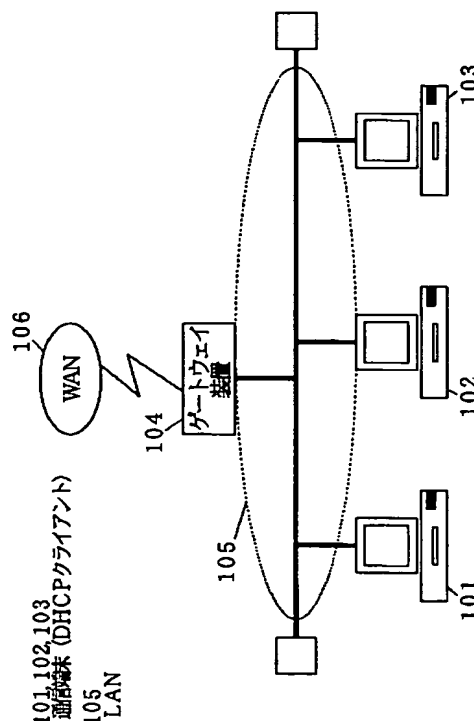
最終頁に続く

(54) 【発明の名称】 鍵交換システム

(57) 【要約】

【課題】 既存の通信プロトコルを利用して、LAN上の複数台の通信端末とゲートウェイ装置とがそれぞれ別個に簡易に鍵データを交換することにより、暗号鍵データを共有することができる鍵交換システムを提供することを目的とする。

【解決手段】 LAN 105 に接続された複数の通信端末 101、102、103 と、LAN および WAN 106 に接続され集線・変換処理を行う DHCP サーバとしてのゲートウェイ装置 104 とを有する鍵交換システムであって、通信端末 101、102、103 は、起動時にネットワーク情報を取得するためにゲートウェイ装置 104 との間で行う DHCP 通信時に、鍵データも同時に交換する。



【特許請求の範囲】

【請求項 1】 LAN に接続された複数の通信端末と、 LAN および WAN に接続され集線・変換処理を行う DHCP サーバとしてのゲートウェイ装置とを有する鍵交換システムであって、

前記通信端末は、起動時にネットワーク情報を取得するために前記ゲートウェイ装置との間で行う DHCP 通信時に、鍵データも同時に交換することを特徴とする鍵交換システム。

【請求項 2】 前記通信端末は、付与されたネットワーク情報の有効期限切れまでに前記ゲートウェイ装置に対して行うネットワーク情報の延長申請要求から始まる DHCP 通信時に、以前交換した共有鍵データを廃棄し、新たに鍵データを交換して共有鍵データを更新することを特徴とする請求項 1 に記載の鍵交換システム。

【請求項 3】 LAN に接続された複数の通信端末と、 LAN および WAN に接続され集線・変換処理を行う DHCP サーバとしてのゲートウェイ装置とを有する鍵交換システムであって、

前記通信端末は、前記ゲートウェイ装置を介して WAN に送信されるデータについてのみ暗号鍵データで通信データを暗号化して LAN に送信し、前記ゲートウェイ装置は、前記送信元の通信端末と共有する暗号鍵データを使用して通信データを復号化して WAN に送信することを特徴とする鍵交換システム。

【請求項 4】 前記ゲートウェイ装置は、WAN から LAN 内の宛先通信端末へのパケットを受信し、前記宛先通信端末と共有する暗号鍵データで通信データを暗号化して LAN に出力し、前記宛先通信端末は、前記ゲートウェイ装置との間で共有する暗号鍵データを使用して復号化することを特徴とする請求項 3 に記載の鍵交換システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、複数の通信端末とその複数の通信端末を接続した LAN とその LAN をインターネットなどの WAN に接続するゲートウェイ装置とで構成され、しかも LAN 内の各通信端末が DHCP (Dynamic Host Configuration Protocol) クライアントとしてネットワーク情報を要求し、ゲートウェイ装置が DHCP サーバとして各通信端末にネットワーク情報を付与して一元管理する LAN システムにおいて、LAN 内通信の秘匿性を確保して WAN との通信を行う鍵交換システムに関するものである。

【0002】

【従来の技術】 近年、インターネットの爆発的に普及に伴い、企業のみならず家庭でも LAN を構築する事例が増えている。また、マンションなどの集合住宅で LAN を構築し、各家庭の端末から LAN 経由でインターネッ

トに接続するなど、これまでの企業で構築されてきたものとは性質の異なる形態の LAN も登場している。こうした形態の場合、インターネットへの接続性のみが重視され、通常の LAN で重要視される情報の共有は必要なくなり、逆に LAN 内でのネットワーク情報の秘匿化が必要になる。また企業などで構築される既存の LAN においても、共有する情報とは別に LAN 内の通信データを暗号化して安全性を確保する需要が高まっている。

【0003】 図 1 は、LAN 内の通信データを暗号化して安全性を確保するための一般的な鍵交換システムを示す構成図である。

【0004】 図 1 において、101～103 は後述の LAN 105 内の通信端末（例えばパソコン）、104 は LAN 105 と後述の WAN 106 との間に介在し、集線・変換処理を行うゲートウェイ装置、105 は通信端末 101～103 とゲートウェイ装置 104 とが接続された LAN、106 はインターネットなどの WAN である。通信端末 101～103 およびゲートウェイ装置 104 が LAN 105 に出力したパケットデータは、LAN 105 内に接続された全ての端末、つまり通信端末 101～103 とゲートウェイ装置 104 とが受信することになる。

【0005】 図 2 は、図 1 に示すゲートウェイ装置と通信端末を詳細に示すブロック図である。

【0006】 図 2 において、201 は LAN 210 及び WAN 209 との間に介在して集線、変換処理を行うゲートウェイ装置であり、ゲートウェイ装置 201 は、ネットワークに接続するインタフェースとして、LAN 210 に接続する LAN 物理接続部と、WAN 209 に接続する WAN 物理接続部 203 とを持ち、その接続の制御をそれぞれ LAN コントローラ 204 と WAN コントローラ 205 が行う。そして、ゲートウェイとしてのルーティング機能はルーティング処理部 206 が行うが、そのためにはネットワーク情報テーブル 208 を参照・登録する必要がある。このネットワーク情報テーブル 208 は記憶装置 207 の内部に構築される。211 は LAN 210 を介して接続される通信端末 211 であり、通信端末 11 は、ネットワークに接続するインタフェースとして、LAN 210 と接続する LAN 物理接続部 212 を持ち、LAN 物理接続部 212 の接続は LAN コントローラ 213 により制御される。通信端末としての機能は通信プロトコル処理部 214 が行うが、そのためにはネットワーク情報テーブル 216 を参照・登録する必要がある。このネットワーク情報テーブル 216 は記憶装置 215 の内部に構築される。

【0007】 次に、DHCP 通信モデルについて図 3 を参照しながら解説する。図 3 は通信端末としての DHCP クライアント 301 と DHCP サーバ 302 との間の通信手順を示すシーケンス図である。図 3 において、301 は DHCP クライアント、302 は DHCP サーバ

である。DHCPはクライアント・サーバモデルの通信プロトコルで、DHCPサーバ302がネットワーク内の通信端末301のIPアドレスなどのネットワーク情報を一元管理するためのメカニズムを提供する。一般的には、LAN上のDHCPサーバ302が、同一セグメント内の通信端末301にIPアドレスなどのネットワーク情報を有効期限付きで付与する形で利用される。

【0008】図3において、まず、通信端末301は、電源起動後にIPアドレス構築のため、LAN内の全端末に向けてDHCPDISCOVERメッセージをブロードキャスト（同報通信）する（S1）。DHCPDISCOVERメッセージを受信したネットワーク内のDHCPサーバ302は、要求された構成情報をDHCP OFFERメッセージにより通知する（S2）。ネットワーク上に複数のDHCPサーバが存在する場合、その全てがDHCP OFFERメッセージを送信し、DHCPクライアント301は複数のDHCP OFFERメッセージを受信することになる。

【0009】DHCP OFFERメッセージを受信したDHCPクライアント301は、複数のDHCPサーバからメッセージを受信した場合は図3ではDHCPサーバ302を選択し、選択したDHCPサーバ302にDHCP REQUESTメッセージを送信し、IPアドレス他のネットワーク情報を要求する（S3）。対するDHCPサーバ302は、DHCPクライアント301からの要求が妥当でそれに応えられる場合は、DHCP ACKメッセージをDHCPクライアント301に送信し、IPアドレスを含むネットワーク情報を付与し、DHCPクライアント301はIP通信が可能になる（S4）。また、この時ネットワーク情報の有効期限も設定される。DHCPクライアント301は、この有効期限内（DHCPの初期設定では有効期間の50%の時間が経過した時点）にDHCPサーバ302にIPアドレス延長申請としてDHCP REQUESTメッセージを送信し（S5）、DHCPサーバ302はこれに対して返信することで（S6）、ネットワーク情報の更新・有効期限延長が行われる。

【0010】次に、通信データの暗号化等で安全性を確保する既存のセキュリティ・プロトコルについて解説する。既存のセキュリティ・プロトコルとして代表的なものにIPsec（Security for Internet Protocol）やPGP（Pretty Good Privacy）などが存在するが、前者はパケットにおけるIP層以降の暗号化／認証を提供するもので、主にゲートウェイ装置に実装され、WAN上におけるVPN確立に利用されている。暗号鍵の管理は、手動鍵管理方式と自動鍵管理方式がある。自動鍵管理方式を実現するためには、IKE（Internet Key Exchange）というIPsec本体とは別にプロトコルを実装しなければならない。後者PG

Pは電子メールの暗号化のみに用いられる。電子メールの暗号化／復号化には公開鍵暗号方式が用いられる。これは利用者が予め自分の公開鍵を鍵サーバに登録しておく。メールの送信者は鍵サーバから送り先の相手の公開鍵を取得し、それを用いてメール内容を暗号化し、送信する。メールの受信者は自分が所有する秘密鍵を用いて暗号化されたメールを復号化する。

【0011】

【発明が解決しようとする課題】しかしながら、上記従来の鍵交換システムでは、LAN内の通信のみを秘匿化することを目的にした通信プロトコルがなく、また2点間で通信データの暗号化／復号化を行う鍵データを共有させることが必要になるが、手動で2点間の鍵データを設定するのは非常に非効率的であるし、自動的に鍵データを共有させるためにも、鍵データ交換を行う通信プロトコルの実装、もしくはそれをサポートした製品の購入が必要となる。

【0012】この鍵交換システムでは、既存の通信プロトコルを利用して、LAN上の複数台の通信端末とゲートウェイ装置とがそれぞれ別個に簡易に鍵データを交換することにより、暗号鍵データを共有することが要求されている。

【0013】本発明は、この要求を満たすため、既存の通信プロトコルを利用して、LAN上の複数台の通信端末とゲートウェイ装置とがそれぞれ別個に簡易に鍵データを交換することにより、暗号鍵データを共有することができる鍵交換システムを提供することを目的とする。

【0014】

【課題を解決するための手段】この課題を解決するために本発明の鍵交換システムは、LANに接続された複数の通信端末と、LANおよびWANに接続され集線・変換処理を行うDHCPサーバとしてのゲートウェイ装置とを有する鍵交換システムであって、通信端末は、起動時にネットワーク情報を取得するためにゲートウェイ装置との間で行うDHCP通信時に、鍵データも同時に交換する構成を備えている。

【0015】この構成により、既存の通信プロトコルを利用して、LAN上の複数台の通信端末とゲートウェイ装置とがそれぞれ別個に簡易に鍵データを交換することにより、暗号鍵データを共有することができる鍵交換システムが得られる。

【0016】

【発明の実施の形態】本発明の請求項1に記載の鍵交換システムは、LANに接続された複数の通信端末と、LANおよびWANに接続され集線・変換処理を行うDHCPサーバとしてのゲートウェイ装置とを有する鍵交換システムであって、通信端末は、起動時にネットワーク情報を取得するためにゲートウェイ装置との間で行うDHCP通信時に、鍵データも同時に交換することとしたものである。

【0017】この構成により、ゲートウェイ装置と各通信端末との間でそれぞれ別個に、2点間で共有鍵暗号方式によって通信データの暗号化／復号化を行う際に使用できる鍵データが簡易に共有されるという作用を有する。

【0018】請求項2に記載の鍵交換システムは、請求項1に記載の鍵交換システムにおいて、通信端末は、付与されたネットワーク情報の有効期限切れまでにゲートウェイ装置に対して行うネットワーク情報の延長申請要求から始まるDHCP通信時に、以前交換した共有鍵データを廃棄し、新たに鍵データを交換して共有鍵データを更新することとしたものである。

【0019】この構成により、LAN内部で定期的に行われるDHCPセッションと鍵データ交換手順を同期させ、LAN内の各通信端末とゲートウェイ装置で共有する暗号鍵データの定期的な更新を確立し、暗号鍵データの安全性を向上させるという作用を有する。

【0020】請求項3に記載の鍵交換システムは、LANに接続された複数の通信端末と、LANおよびWANに接続され集線・変換処理を行うDHCPサーバとしてのゲートウェイ装置とを有する鍵交換システムであって、通信端末は、ゲートウェイ装置を介してWANに送信されるデータについてのみ暗号鍵データで通信データを暗号化してLANに送信し、ゲートウェイ装置は、送信元の通信端末と共有する暗号鍵データを使用して通信データを復号化してWANに送信することとしたものである。

【0021】この構成により、WANへの送信性を損なうことなくLAN内の通信のみを暗号化して秘匿化が実現されるという作用を有する。

【0022】請求項4に記載の鍵交換システムは、請求項3に記載の鍵交換システムにおいて、ゲートウェイ装置は、WANからLAN内の宛先通信端末へのパケットを受信し、宛先通信端末と共有する暗号鍵データで通信データを暗号化してLANに出力し、宛先通信端末は、ゲートウェイ装置との間で共有する暗号鍵データを使用して復号化することとしたものである。

【0023】この構成により、WANからの受信性を損なうことなくLAN内の通信のみを暗号化して秘匿化が実現されるという作用を有する。

【0024】以下、本発明の実施の形態について図1～図10を用いて説明する。

【0025】(実施の形態1) 本発明の実施の形態1による鍵交換システムの構成は図1、図2と同様であるので、その説明は省略する。本実施の形態と従来の技術とが異なるところは、ゲートウェイ装置としてのDHCPサーバとパソコン等の通信端末(DHCPクライアント)の機能、動作等に関する点である。

【0026】このような構成の鍵交換システムについて、図1、図3～図8を用いて説明する。図4(a)、

(b)はDHCP通信によって付与されるデータの詳細を示すデータ図であり、図4(a)はDHCPデータ構造の詳細を示し、図4(b)はDHCPサーバから付与される主なネットワーク情報の項目を示す。また、図5はDiffie-Hellman方式による鍵交換の説明図であり、図6は一方の通信端末Aの動作を示すフローチャート、図7は他方の通信端末Bの動作を示すフローチャート、図8はDHCPクライアントとしての通信端末とDHCPサーバとしてのゲートウェイ装置との間の通信シーケンスを示すシーケンス図である。図8において、601はDHCPクライアントとなる通信端末、602はDHCPサーバとなるゲートウェイ装置である。

【0027】図1において、LAN105に接続する通信端末101～103は、起動時に図4(b)に列挙したネットワーク情報を取得するために、DHCPサーバであるゲートウェイ装置104とDHCP通信を行う。この際に同時に、図4(a)のDHCPメッセージにおけるオプションフィールド(オプション部)を利用し、Diffie-Hellman(ディフィー・ヘルマン)の鍵交換方式によって、通信端末101～103とゲートウェイ装置104との間で個別に暗号鍵を共有する。

【0028】図5において、A、BはDiffie-Hellman方式を用いて鍵交換を行う通信端末で、まず鍵交換を始める前に、通信端末A、B間であらかじめ素数である p と、 $1 < \alpha < p$ となる適当な整数 α を決めておく必要がある。 p と α はA、B以外の第三者に知られてもよい。次に、通信端末Aは適当な正の整数 X_a を選び、図6に示すように(数1)を計算し(S11)、鍵データ Y_a をBに送信する(S12)(なお、 mod とは割り算の剰余の表現のことであり、例えば $17 \text{ mod } 7$ とは17を7で割った余りのことである)。

【0029】

【数1】

$$Y_a = \alpha^{X_a} \text{ mod } p$$

【0030】この時、通信端末A以外の他者に X_a を知られてはいけない(X_a は秘密鍵といわれる)。同様に通信端末Bは適当な正の整数 X_b を選び、図7に示すように(数2)を計算し(S21)、鍵データ Y_b をAに送信する(S22)。

【0031】

【数2】

$$Y_b = \alpha^{X_b} \text{ mod } p$$

【0032】 X_a と同様に X_b も通信端末B以外の他者に知られてはならない(X_b は秘密鍵データといわれる)。通信端末Aは、通信端末Bから受信した Y_b を使用して、(数3)を計算し(S13)、共有鍵データ K_{ab} を求めることができる。

【0033】

【数3】

$$K_{ab} = Y_b^{X_a} \bmod p \\ = \alpha^{X_a X_b} \bmod p$$

【0034】また通信端末Bも、(数4)を計算することと同様に共有鍵データ K_{ab} を求めることができる(S23)。

【0035】

【数4】

$$K_{ab} = Y_a^{X_b} \bmod p \\ = \alpha^{X_a X_b} \bmod p$$

【0036】次に、DHCP通信とDiffie-Hellman方式とを組み合わせた鍵交換システムについて図8で説明する。

【0037】DHCPクライアント601は起動時、IPアドレスなどのネットワーク情報を取得するため、DHCPDISCOVERメッセージをLAN内にブロードキャストする(S31)。DHCPDISCOVERメッセージを受信したDHCPサーバ602は、素数 p と $1 < \alpha < p$ となる適当な正の整数 α を決定し、DHCPデータ構造におけるオプション部(図4(a)参照)に格納し、DHCPOFFERメッセージとして返信する(S32)。 p 、 α は第三者に知られてもよい情報なので、平文(DHCP通信における通常の文章データ)のまま通信路にのせても問題ない。

【0038】DHCPOFFERメッセージを受信したDHCPクライアント601は、 p と α を受信する。もしLAN内に複数のDHCPサーバが存在していても、DHCPデータのオプション部に p と α が格納されているかどうかでDHCPサーバを選択可能である。通信端末601は適当な正の整数である秘密鍵データ X_a を決定し、鍵データ Y_a を算出する。

【0039】また同様にゲートウェイ装置502も、適当な正の整数である秘密鍵データ X_b を決定し、鍵データ Y_b を算出する。DHCPサーバを決定したDHCPクライアント601は、DHCPREQUESTメッセージを送信し(S33)、ネットワーク情報をDHCPサーバ602に要求するが、このときDHCPデータのオプション部に独自に算出した Y_a を格納しておく。

【0040】DHCPREQUESTメッセージを受信したDHCPサーバ602は、通信端末601に付与するネットワーク情報をDHCPACKメッセージに格納し、返信する(S34)。このとき独自に算出しておいた Y_b もDHCPデータのオプション部に格納しておく。ここに至ってDHCPクライアント601、DHCPサーバ602の両者とも共有鍵データ K_{ab} を算出可能であり、通信端末601とゲートウェイ装置602との間で、通信データの暗号化/復号化を行う鍵データを安全に交換・共有できたことになる。

【0041】以上のように本実施の形態では、通信端末

601は、起動時にネットワーク情報を取得するためにゲートウェイ装置602との間で行うDHCP通信時に、鍵データ Y_a 、 Y_b も同時に交換するようにしたことにより、ゲートウェイ装置602と各通信端末601との間でそれぞれ別個に、2点間で共有鍵暗号方式によって通信データの暗号化/復号化を行う際に使用できる鍵を簡易に共有することができる。

【0042】(実施の形態2)本発明の実施の形態2による鍵交換システムの構成は図1、図2と同様であるので、その説明は省略する。本実施の形態と従来の技術とが異なるところは、ゲートウェイ装置としてのDHCPサーバとパソコン等の通信端末の機能、動作等に関する点である。

【0043】このような構成の鍵交換システムについて、図1、図4、図8を用いて説明する。

【0044】図4(b)に示すように、DHCP通信によって付与されるデータには、IPアドレスやネットマスクの他に、付与したネットワーク情報の有効期限(貸し出し有効期限)というものがあり、DHCPクライアントは付与された有効期限内(初期設定では有効期限の50%)にDHCPサーバと通信し、ネットワーク情報の再取得を行う。図3に示すように、ネットワーク情報の再取得は、DHCPDISCOVER、DHCPOFFERメッセージの送受信は必要なく、DHCPREQUEST、DHCPACKメッセージの送受信のみで行われる(ステップS5、S6参照)。ネットワーク情報の再取得に関しては、IPアドレスなど以前取得した情報を基本的にはできる限りそのまま保持する形で行われるが、共有鍵データはネットワーク情報再取得の際に内容を更新するようにして、共有鍵データの安全性を高める。

【0045】このような共有鍵データの更新について、ネットワーク情報再取得時の鍵情報更新手順を示す図8を用いて説明する。

【0046】図8に示すように、ネットワーク再取得のトリガがDHCPクライアント601にかかる、以前使用した秘密鍵データ X_a を廃棄し、新たに正の整数である秘密鍵データ X_a を再設定し、鍵データ Y_a を算出する。そして、DHCPサーバ602に対してDHCPREQUESTメッセージを送信する(S35)。この際、DHCPデータのオプション部に再計算した鍵データ Y_a を格納しておく。DHCPクライアント601からのDHCPREQUESTメッセージを受信したDHCPサーバ602は、以前使用した秘密鍵データ X_b を廃棄し、新たに正の整数である秘密鍵データ X_b を再設定し、鍵データ Y_b を算出する。そして、DHCPクライアント601に対してネットワーク情報を付与するDHCPACKメッセージを送信するが(S36)、DHCPデータのオプション部に鍵データ Y_b を格納しておく。ここに至ってDHCPクライアント(通信端末)6

01、DHCPサーバ（ゲートウェイ装置）602の両者とも新しい共有鍵データKabを算出可能であり、通信端末601とゲートウェイ装置602の間で通信データの暗号化／復号化を行う鍵を更新できたことになる。

【0047】以上のように本実施の形態では、通信端末601は、付与されたネットワーク情報の有効期限切れまでにゲートウェイ装置602に対して行うネットワーク情報の延長申請要求から始まるDHCP通信時に、以前交換した共有鍵データを廃棄し、新たに鍵データを交換して共有鍵データを更新するようにしたことにより、LAN内部で定期的に行われるDHCPセッションと鍵交換手順を同期させ、LAN内の各通信端末601とゲートウェイ装置602で共有する暗号鍵データの定期的な更新を確立して、暗号鍵データの安全性を向上させることができる。

【0048】（実施の形態3）本発明の実施の形態3による鍵交換システムの構成は図1、図2と同様であるので、その説明は省略する。本実施の形態と従来の技術とが異なるところは、ゲートウェイ装置としてのDHCPサーバとパソコン等の通信端末の機能、動作等に関する点である。

【0049】このような構成の鍵交換システムについて、図9、図10を用いて説明する。図9はLAN内における暗号化通信のイメージ図であり、図10（a）は通信端末701が保持するネットワーク情報と鍵情報の管理テーブルを示すテーブル図、図10（b）はゲートウェイ装置704が保持するネットワーク情報と鍵情報の管理テーブルを示すテーブル図である。

【0050】図9において、701～703は後述のLAN709内の通信端末、704はゲートウェイ装置、705はインターネットなどのWAN、706、707、708はゲートウェイ装置704と通信端末701、通信端末702、通信端末703との間で暗号鍵データ（それぞれK1、K2、K3）を共有することで構築されるVPN、709はLANである。

【0051】図9において、通信端末701がWAN705に向けてパケットを送信する場合、ゲートウェイ装置704がパケットを中継（ルーティング）する。通信端末701は、保持するネットワーク情報と鍵情報の管理テーブルをみると、ゲートウェイ装置704との間で暗号鍵データK1を共有しているので、暗号鍵データK1を用いてパケットを暗号化し、LAN709上に送信する。通信端末701からゲートウェイ装置704へのパケットはLAN709に接続する全端末が受信可能であるが、通信端末701とゲートウェイ装置704の2点間のみで共有される暗号鍵データK1で暗号化されているため、通信端末701とゲートウェイ装置704との間で構築されたVPN706上を流れているものとみなすことが可能である。暗号化済みパケットを受信したゲートウェイ装置704は、パケットの送信元MACア

ドレスを保持するネットワーク情報と鍵情報の管理テーブルで検索し、暗号鍵データK1により暗号化されていることが分かるので、共有暗号鍵データK1でパケットを復号化し、WAN705にパケットを送信する。

【0052】また、逆にWAN705からLAN709内の通信端末701宛てのパケットをゲートウェイ装置704が受信した場合、宛先のIPアドレスと保持するネットワーク情報、鍵情報管理テーブルで検索し、宛先が通信端末701であることと通信端末701との間で暗号鍵データK1を共有していることが分かる。そこで、ゲートウェイ装置704は、暗号鍵データK1を使用してパケットを暗号化し、LAN709に送信する。通信端末701は、宛先MACアドレスが自身のものであるため、送信元のMACアドレスを保持するネットワーク情報、鍵情報管理テーブルで検索し、暗号鍵データK1を共有しているので、暗号鍵データK1を用いてパケットを復号化する。通信端末702、703も通信端末701宛てのパケットを受信することはできるが、暗号化／復号化鍵が異なるので正しく復号はできず、通信端末701とゲートウェイ装置704との間で構築されたVPN706上をデータが流れているものと考えることができる。以上のようにして、LAN709内の上り／下りの両方についてデータの秘匿化を実現することができる。

【0053】以上のように本実施の形態では、通信端末701は、ゲートウェイ装置704を介してWAN705に送信されるデータについてのみ暗号鍵データで通信データを暗号化してLAN709に送信し、ゲートウェイ装置704は、送信元の通信端末701と共有する暗号鍵データK1を使用して通信データを復号化してWAN705に送信するようにしたことにより、WAN705への送信性を損なうことなくLAN709内の通信のみを暗号化して秘匿化を実現することができる。

【0054】また、ゲートウェイ装置704は、WAN705からLAN709内の宛先通信端末701へのパケットを受信し、宛先通信端末701と共有する暗号鍵データK1で通信データを暗号化してLAN709に出力し、宛先通信端末701は、ゲートウェイ装置704との間で共有する鍵データを使用して復号化するようにしたことにより、WAN705からの受信性を損なうことなくLAN709内の通信のみを暗号化して秘匿化を実現することができる。

【0055】

【発明の効果】以上説明したように本発明の請求項1に記載の鍵交換システムによれば、LANに接続された複数の通信端末と、LANおよびWANに接続され集線・変換処理を行うDHCPサーバとしてのゲートウェイ装置とを有する鍵交換システムであって、通信端末は、起動時にネットワーク情報を取得するためにゲートウェイ装置との間で行うDHCP通信時に、鍵データも同時に

交換することにより、ゲートウェイ装置と各通信端末との間でそれぞれ別個に、2点間で共有鍵暗号方式によって通信データの暗号化／復号化を行う際に使用できる鍵データを簡易に共有することができるという有利な効果が得られる。

【0056】請求項2に記載の鍵交換システムによれば、請求項1に記載の鍵交換システムにおいて、通信端末は、付与されたネットワーク情報の有効期限切れまでにゲートウェイ装置に対して行うネットワーク情報の延長申請要求から始まるDHCP通信時に、以前交換した共有鍵データを廃棄し、新たに鍵データを交換して共有鍵データを更新することにより、LAN内部で定期的に行われるDHCPセッションと鍵データ交換手順を同期させ、LAN内の各通信端末とゲートウェイ装置で共有する暗号鍵データの定期的な更新を確立し、暗号鍵データの安全性を向上させることができるという有利な効果が得られる。

【0057】請求項3に記載の鍵交換システムによれば、LANに接続された複数の通信端末と、LANおよびWANに接続され集線・変換処理を行うDHCPサーバとしてのゲートウェイ装置とを有する鍵交換システムであって、通信端末は、ゲートウェイ装置を介してWANに送信されるデータについてのみ暗号鍵データで通信データを暗号化してLANに送信し、ゲートウェイ装置は、送信元の通信端末と共有する暗号鍵データを使用して通信データを復号化してWANに送信することにより、WANへの送信性を損なうことなくLAN内の通信のみを暗号化して秘匿化を実現することができるという有利な効果が得られる。

【0058】請求項4に記載の鍵交換システムによれば、請求項3に記載の鍵交換システムにおいて、ゲートウェイ装置は、WANからLAN内の宛先通信端末へのパケットを受信し、宛先通信端末と共有する暗号鍵データで通信データを暗号化してLANに出力し、宛先通信端末は、ゲートウェイ装置との間で共有する暗号鍵データを使用して復号化することにより、WANからの受信性を損なうことなくLAN内の通信のみを暗号化して秘匿化を実現することができるという有利な効果が得られる。

【図面の簡単な説明】

40

【図1】一般的な鍵交換システムを示す構成図

【図2】図1に示すゲートウェイ装置と通信端末を詳細に示すブロック図

【図3】通信端末としてのDHCPクライアントとゲートウェイ装置としてのDHCPサーバとの間の通信手順を示すシーケンス図

【図4】(a) DHCP通信によって付与されるデータの詳細を示すデータ図

(b) DHCP通信によって付与されるデータの詳細を示すデータ図

【図5】Diffie-Hellman方式による鍵交換の説明図

【図6】一方の通信端末の動作を示すフローチャート

【図7】他方の通信端末Bの動作を示すフローチャート

【図8】DHCPクライアントとしての通信端末とDHCPサーバとしてのゲートウェイ装置との間の通信シーケンスを示すシーケンス図

【図9】LAN内における暗号化通信のイメージ図

【図10】(a) 通信端末が保持するネットワーク情報と鍵情報の管理テーブルを示すテーブル図

(b) ゲートウェイ装置が保持するネットワーク情報と鍵情報の管理テーブルを示すテーブル図

【符号の説明】

101、102、103、211、301、601、701、702、703 通信端末 (DHCPクライアント)

104、291、302、602、704 ゲートウェイ装置 (DHCPサーバ)

105、210、709 LAN

106、209、705 WAN

202、212 LAN物理接続部

203 WAN物理接続部

204、213 LANコントローラ

205 WANコントローラ

206 ルーティング処理部

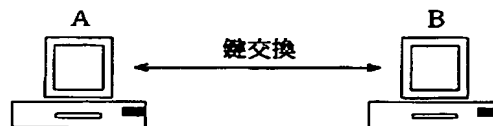
207、215 記憶装置

208、216 ネットワーク情報テーブル

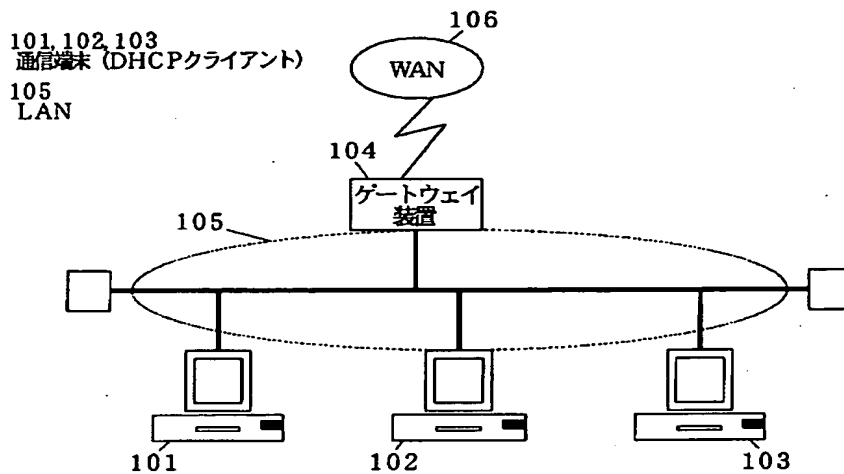
214 通信プロトコル処理部

706、707、708 VPN

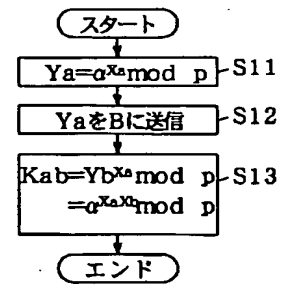
【図5】



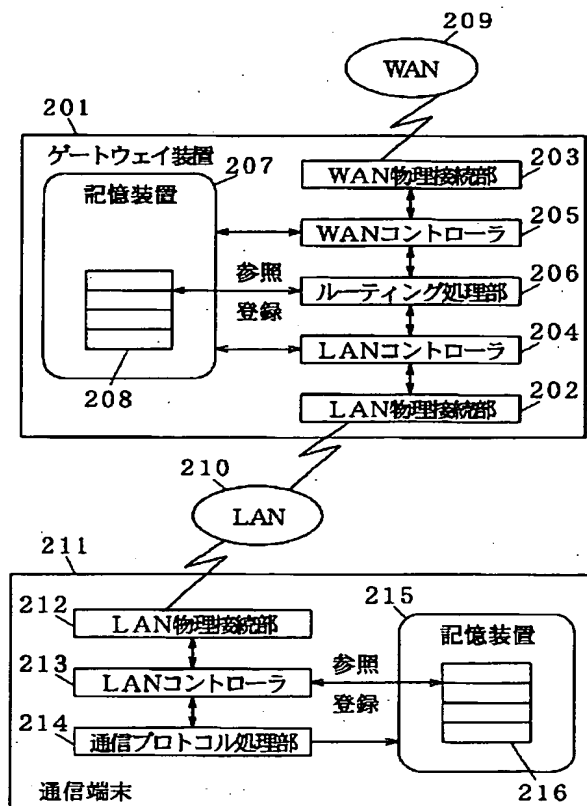
【図1】



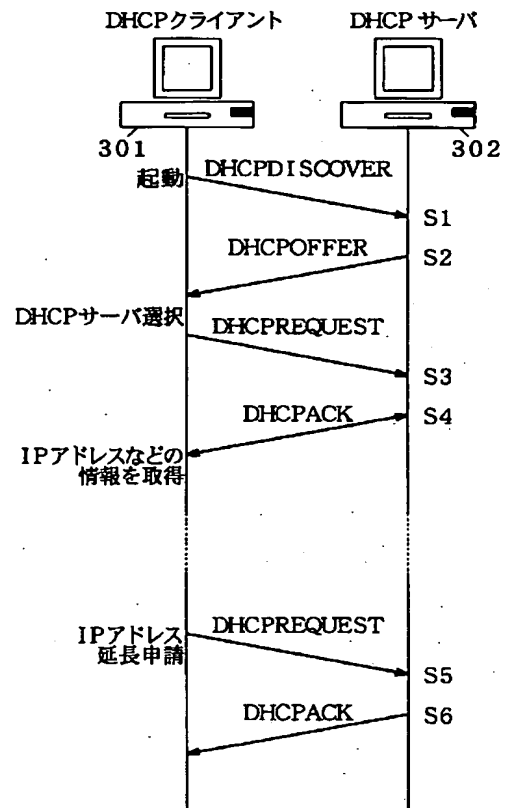
【図6】



【図2】



【図3】



【図4】

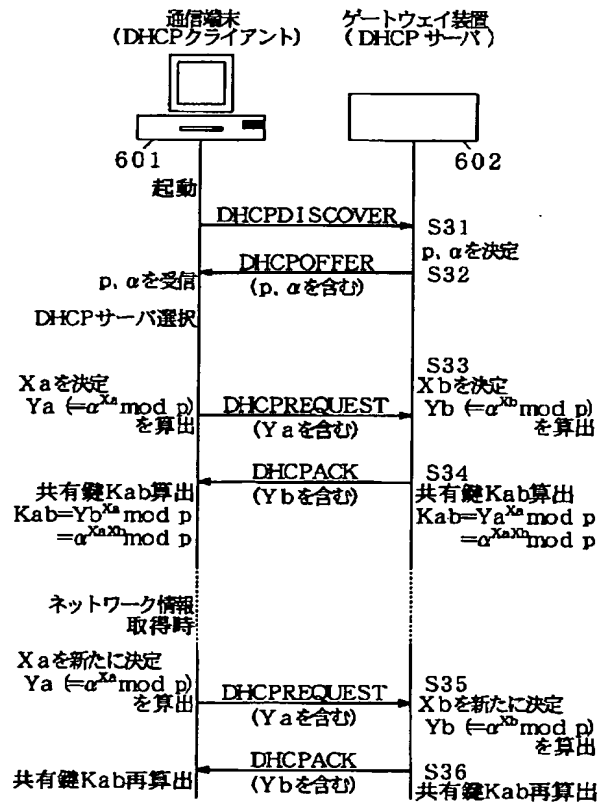
(a)

operation code(1)	ハードウェア番号(1)	ハードウェアアドレス(1)	転送回数(1)
トランザクションID(4)			
経過時間(2)		ブロードキャストフラグ(2)	
クライアントIPアドレス(4)			
要求者IPアドレス(4)			
サーバIPアドレス(4)			
リレーエージェントIPアドレス(4)			
クライアントMACアドレス(16)			
サーバのホスト名(64)			
ブートファイル名(128)			
オプション(可変長)			

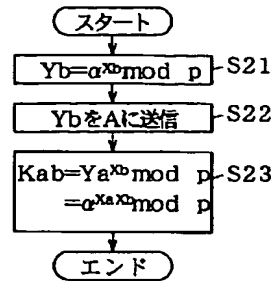
(b)

・IPアドレス
・ネットマスク
・デフォルトゲートウェイIPアドレス
・貸し出し有効期限
・ドメインネームサーバアドレス
・ドメイン名

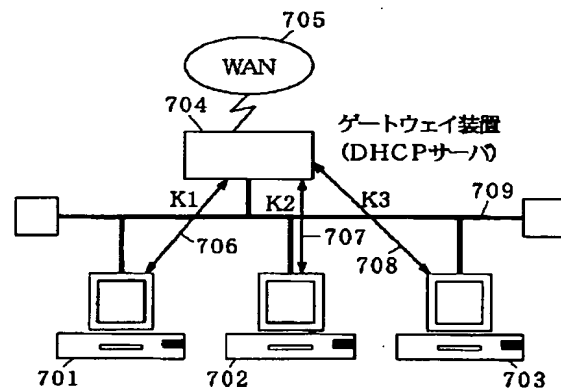
【図8】



【図7】



【図9】



【図10】

(a)

MACアドレス	IPアドレス	秘密鍵	共有鍵
aa:aa:aa:aa:aa:aa	192.168.0.X	Xa	K1

(b)

MACアドレス	IPアドレス	秘密鍵	共有鍵
aa:aa:aa:aa:aa:aa	192.168.0.X	X1	K1
yy:yy:yy:yy:yy:yy	192.168.0.b	X2	K2
zz:zz:zz:zz:zz:zz	192.168.0.c	X3	K3

フロントページの続き

- Fターム(参考) 5J104 AA16 BA02 EA24 EA28 EA33
NA03 PA07
5K030 GA15 HD03 HD06 JT02 LD19
5K033 AA08 CB08 CC01 DB10 DB18
9A001 BB04 CC03 CC08 DD10 EE03
JJ13 JJ14 JJ25 JJ27 KK56
LL03

THIS PAGE BLANK (SP'0)